Nom : Prénom :

DS Sécurité réseau – 12 Février 2020

Documents et calculatrices interdites

1. Nous supposons un chiffrement symétrique. Le mot de passe est e761 en hexadécimal. Le mot/nombre à déchiffrer est 2c10.

Réponse :

□ ab41 □ 1b31 □ ca21 □ cb4d □ cb41 □ cb71

□ cb42 □ 1234 □ abcd □ ed65 □ ed64 □ a311

Algorithme RSA

Rappel : (p,q) deux nombres premiers. N=p*q et phi=(p-1)*(q-1). e premier avec phi et d choisit de manière à avoir e*d mod(phi)=1. Dans la suite, nous considérons les deux entiers (p,q)=(5,11).

2. Cochez les valeurs possibles pour e (parmi celles-ci-dessous):

□ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8

□ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15

3. Pour e =23, donnez la valeur de d (1 seule réponse):

□ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8

□ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15

4. Quelle est la clé publique ?

□ (11,34) □ (11,55) □ (7,55) □ (13,40) □ (7,40) □ (9,40)

□ (23,40) □ (23,55) □ (12,55) □ (12,40) □ (5,40) □ (5,55)

5. Quelle est la clé privée ?

□ (11,34) □ (11,55) □ (7,55) □ (13,40) □ (7,40) □ (9,40)

□ (23,40) □ (23,55) □ (12,55) □ (12,40) □ (5,40) □ (5,55)

6. Quel est le résultat du chiffrement de la valeur 2 par la clé privée ?

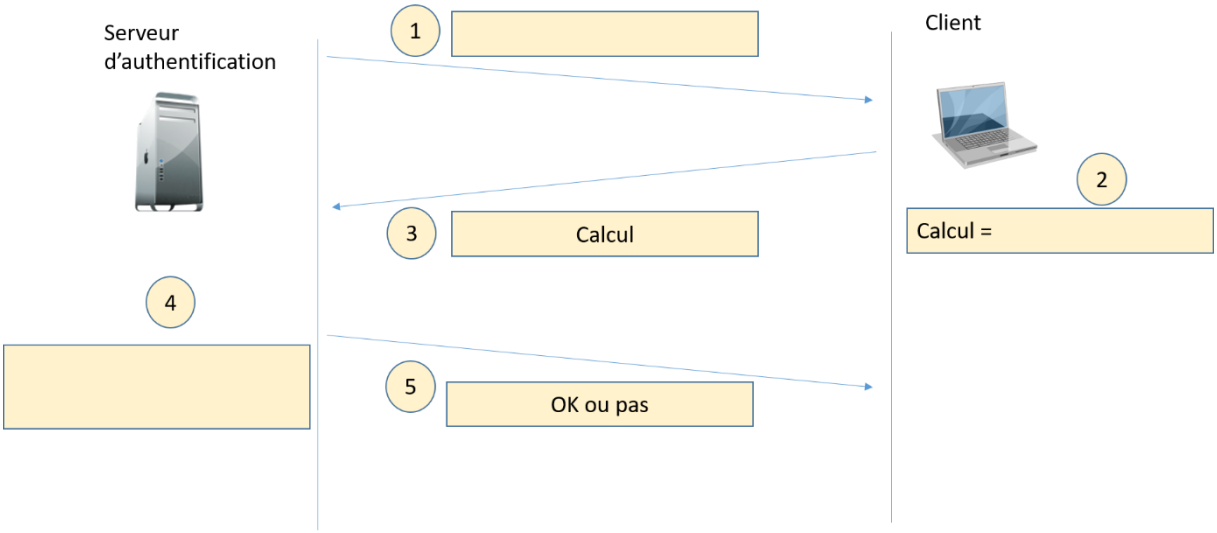
□ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8

□ 9 □ 10 □ 18 □ 12 □ 13 □ 14 □ 15

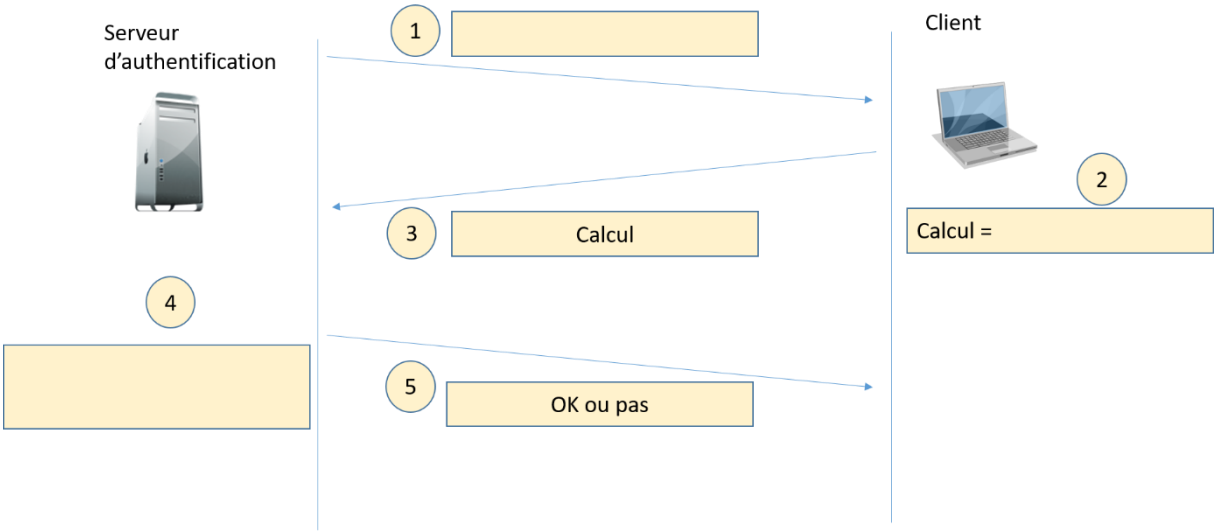
Authentification

7. Nous souhaitons authentifier un utilisateur à partir de mots de passes (clés symétriques) partagées par le client et le serveur. Complétez les différentes opérations ci-dessous.

Nom : Prénom :



8. Même question pour un chiffrement asymétrique. Attention de bien différencier clé publique et clé privée.



9. Quels sont les avantages et inconvénients du chiffrement symétrique ?

10. Quels sont les avantages et inconvénients du chiffrement asymétrique ?